UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/634,117	08/04/2003	James M. Doherty	1033-T00534	5753

60533 7590 08/17/2007

TOLER SCHAFFER, LLP
8500 BLUFFSTONE COVE
SUITE A201
AUSTIN, TX 78759

EXAMINER	
HOANG, DANIEL L	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/634,117
Filing Date: August 04, 2003
Appellant(s): DOHERTY ET AL.

Jeffrey G, Toler, Reg. No. 38,342
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/28/07 appealing from the Office action mailed 10/18/06.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20040049693	Douglas	9-2002
6081894	Mann	10-1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Douglas (US PGP 20040049693) and further in view of Mann (US Patent No. 6,081,894).

With respect to claim 1, Douglas teaches:

A method comprising:

providing a host computer system having at least one network interface interfaced with a computer network; **(see figure 1A)**

operating the host computer system in a multi-user mode; **(see figure 1A)**

detecting an intrusion event using a system daemon; **(see figure 2, element 22).**

Douglas does not expressly disclose responding to the detection of the intrusion event by isolating at least one network interface from the computer network and limiting physical access to the host computer system by taking the host computer down to a single user state.

Mann teaches:

In response to detecting the intrusion event, isolating at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system **(column 3, lines 2-5).**

It would have been obvious at the time that the invention was made to a person of ordinary skill in the art to which the subject matter pertains to modify Douglas' invention so that when an intrusion is detected on the host system, the host can be isolated from the remote devices in order to prevent propagation of the intrusion.

With respect to claims 3 and 4, the Douglas reference discloses his invention's capability of being implemented on UNIX platforms. The Douglas reference does not expressly disclose isolating the network by issuing an IFCONFIG down command or taking down the host computer system by issuing an INIT1 command. It was well recognized to those of ordinary skill in the pertinent arts that IFCONFIG and INIT1 are UNIX commands used to shut down network interfaces and taking machines offline, respectively. Because the Douglas reference discloses UNIX, it would have been obvious to one of ordinary skill in the art to use the built-in IFCONFIG and INIT1 functions to shut down network interfaces and take machines offline.

With respect to claim 5, Douglas teaches:

Reading, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion. **(see figure 2, elements 22 and 22b)**

With respect to claim 6, Douglas teaches:

A directive type that indicates a file to be monitored for intrusion, **(see paragraph 57, module 22b)**

A directive type that indicates a directory whose members are to be monitored for intrusion, **(see figure 13A, "/etc/passwd", system is capable of scanning user directories),** and

A directive type that indicates another configuration file to be monitored for intrusion **(see figure 11A-11C, myfconfigfile.cfg, dragon.cfg).**

With respect to claim 7 and 8, Douglas teaches:

Computing a data verification signature for a monitored file in a file system of the host computer system', and comparing the data verification signature to a valid data verification signature for the monitored file; wherein said detecting the intrusion event comprises detecting that the data verification signature differs from the valid data verification signature. **(see paragraphs 105 and 106)**

Douglas also teaches the above wherein the valid data verification signature comprises a Message Digest 5 (MD5) signature. **(see paragraphs 105 and 106)**

With respect to claim 9, Douglas teaches:

Reading the valid data verification signature for the monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system. **(see paragraph 56, lines 10-18)**

With respect to claim 10, Douglas teaches:

Writing a log of the intrusion event to a log database that is not located on the host computer system or second computer system. **(see paragraph 40)**

With respect to claim 11, Douglas teaches:

Detecting an incorrect permission associated with a file in a file system of the host computer system. **(see paragraph 94)**

With respect to claim 12, Douglas teaches:

Detecting an incorrect ownership associated with a file in a tile system of the host computer system. **(see paragraphs 97 and 98)**

With respect to claim 13, Douglas teaches:

Detecting that a file no longer exists in a file system of the host computer system. **(see paragraph 96)**

Claim 14 is rejected by Douglas and Mann as applied to claims 1-8 and 10.

Claim 15 is rejected by Douglas and Mann as applied to claim 1.

Claim 16 is rejected by Douglas and Mann as applied to claim 2.

Claim 17 is rejected by Douglas and Mann as applied to claim 3.

Claim 18 is rejected by Douglas and Mann as applied to claim 4.

Claim 19 is rejected by Douglas and Mann as applied to claim 5.

Claim 20 is rejected by Douglas and Mann as applied to claim 6.

Claim 21 is rejected by Douglas and Mann as applied to claim 7.

Claim 22 is rejected by Douglas and Mann as applied to claim 8.

Claim 23 is rejected by Douglas and Mann as applied to claim 9.

Claim 24 is rejected by Douglas and Mann as applied to claim 10.

Claim 25 is rejected by Douglas and Mann as applied to claim 11.

Claim 26 is rejected by Douglas and Mann as applied to claim 12.

Claim 27 is rejected by Douglas and Mann as applied to claim 13.

(10) Response to Argument

I) Arguments with respect to claims 1 and 3-13 being allowable over Douglas and Mann.

Appellant's first argument concerns the cited reference Mann's failure to disclose "isolating at least one network interface from a computer network and taking a host system down to a single user state so that access to the host computer is limited to physical access at the host computer system." Appellant further argues that Mann teaches that the data sending entity is isolated from the data receiving entity without disrupting normal operation of either entity. Appellant further argues altering the state of the device from a multi-user state to a single user state is a disruption of normal operation. Examiner respectfully disagrees with the appellant's contentions.

Regarding the limitation of "normal operation," Mann only states that normal operation of either entity is not disrupted. Mann does not further distinctly define the exact state of normal operations. Appellant's interpretation of what normal operation seeks to limit the Mann reference but is insufficient to traverse the rejection. Further, it seems from the above argument from appellant, appellant is admitting that Mann teaches altering the state of the device from a multi-user state to a single user state. This is contradictory to appellant's later argument that Mann does not take the host computer system down to a single user state.

Regarding the limitation of "taking the host computer system down to a single user state," the claimed invention claims a host computer system interfaced with a computer network. It is further claimed that the host computer system operates in a multi-user mode that is capable of being taken down to a single user mode. Within the Mann reference, examiner is interpreting the apparatus comprising the data receiving entity, such as a personal computer or even a local area network, as the claimed host computer system. The apparatus is capable of evaluating data received from a data sending entity, such as the Internet. This communication between the computer and the Internet is being interpreted as operating in multi-user mode. Mann further teaches that when a virus in the incoming data stream, power is cut off to prevent passage of data. Thus communication between the host computer and the Internet is stopped. The computer is clearly operating in single user mode as it no longer communicates with the Internet. See col. 3, lines 43-50.

In response to appellant's argument that

> *"The assumption that 'it is clear that both entities are in single user states' is incorrect and not applicable, since neither the 'data isolator' nor the 'data receiving entity of Mann are indicated to be in multi-user state. So it is unclear how the data sending entity could ever be reduced to a single user state."*

Examiner respectfully disagrees. As explained above, the combination of the personal computer and the Internet is viewed as a system communicating in multi-user state. The isolation of the computer from the Internet results in the computer operating in a single user state.

As per Appellant's argument that Mann provides no indication that the personal computer operates in multi-user mode and provides no indication that the data isolator is adapted to take the receiving device down to a single user state. Argument is not persuasive. Mann does provide indication that the data isolator is adapted to take the receiving device down to a single user state. See col. 3, lines 43-50.

Appellant concerns that in regards to dependent claim 4, the asserted combination of Douglas and Mann fails to disclose or suggest that "taking the host computer down to a single user state comprises issuing an INIT1 command to an operating system of the host computer system." Instead, neither Douglas or Mann disclose taking the host computer down to a single user state. To the extent that Mann discloses isolation, such isolation is achieved by activating a data isolator without issuing commands to a host computer system. The examiner disagrees with appellant's contention. It has been discussed above how Mann discloses taking the host computer system down to a single user state. In regards to issuing commands to a host computer system to take the system down to a single user state, examiner would like to point appellant to column 3, lines 43-47 of the Mann reference. Mann teaches that when a virus is detected, a control line from the processor causes the power up control logic circuit to cause the power supply conditioning ISO drive to cut off power to the optical isolator, thereby causing the optical isolator to prevent passage of data. The optical isolator is deemed part of the host computer system and the commands issued to it cause it to take the host computer system down to a single user state.

II) Arguments with respect to claims 15 and 17-27 being allowable over Douglas and Mann.

The appellant's argument concerns the cited references', Douglas and Mann, failure to disclose, "isolating the sending and receiving entities without disrupting normal operation" and "single user state" for the sending or the receiving entities. Moreover, Mann fails to disclose or suggest that the data isolation apparatus can operate in a multi-user mode. Appellant further argues, "Thus, the asserted combination of Douglas and Mann does not disclose or suggest each and every element of claim 15, or of claims 17-27 at least by virtue of their dependency from claim 15." Examiner respectfully disagrees with appellant's contentions.

Regarding the limitation of isolation without disruption of normal operation, Mann only states that normal operation of either entity is not disrupted. Mann does not further distinctly define the exact state of normal operations. Appellant's interpretation of what normal operation seeks to limit the Mann reference but is insufficient to traverse the rejection. Further, it seems from the above argument from appellant, appellant is admitting that Mann teaches altering the state of the device from a multi-user state to a single user state. This is contradictory to appellant's later argument that Mann does not take the host computer system down to a single user state.

Regarding the limitation of operating in a multi-user mode and reducing to a single user state, the combination of the personal computer and the Internet is viewed as a system communicating in multi-user state. The isolation of the computer from the Internet results in the computer operating in a single user state.

III) Arguments with respect to claim 14 being allowable over Douglas and Mann.

Appellant argues that the combination of Douglas and Mann fails to disclose or suggest a method that includes "operating the host computer system in a multi-user mode" and "in response to detecting the intrusion event," "issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state," as recited in claim 14. Examiner respectfully disagrees. The combination of the personal computer and the Internet is viewed as a system communicating in multi-user state. In regards to issuing commands to a host computer system to take the system down to a single user state, examiner would like to point appellant to column 3, lines 43-47 of the Mann reference. Mann teaches that when a virus is detected, a control line from the processor causes the power up control logic circuit to cause the power supply conditioning ISO drive to cut off power to the optical isolator, thereby causing the optical isolator to prevent passage of data. The optical isolator is deemed part of the host computer system and the commands issued to it cause it to take the host computer system down to a single user state..

Appellant further argues that Mann provides no indication that any of the sending entity, the receiving entity, or the data isolator operates in multi-user mode nor that the data isolator is adapted to take the receiving device down to a single user state. Examiner respectfully disagrees. The combination of the personal computer and the Internet is viewed as a system communicating in multi-user state. The isolation of the computer from the Internet results in the computer operating in a single user state. Further, Mann does provide indication that the data isolator is adapted to take the receiving device down to a single user state. See col. 3, lines 43-50.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Daniel L. Hoang

8/02/07

Conferees:

Nasser Moazzami N. M.

Kim Vu KVu

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/15/07